METHOD OF TEMPLATE HIDING DATA IN VECTOR IMAGES

In this work authors propose the new steganographic method of template hiding data in vector image structure. According to the proposed method, hiding data is performed by the gradually separation of Bezier curves into visually identical pluralities of segments with using preassigned correlation table of the different values of template elements with the different steps of Bezier curves structure. There was conducted the software implementation of proposed method of hiding information in vector images of SVG format. The obtained results of experiment were compared with the results of existing bitwise method of hiding data in Bezier curves. The proposed method showed the profit (in more than 2 times) in reduction of steganocontainer size and time, required for hiding data in SVG image structure.

Key words: information security, steganography, vector images, method of template hiding data, method of bitwise hiding data, SVG images, Bezier curves, algorithm de Casteljau.

Ковтун Владислав Юрійович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: vladislav.kovtun@gmail.com.
Ковтун Владислав Юрьевич, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Vladislav Kovtun, Ph.D., docent of Academic Department of IT-Security, National Aviation University.

Кінзерявий Олексій Миколайович, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: oleksiykinzeryavyy@gmail.com.
Кинзерявый Алексей Николаевич, аспирант кафедры безопасности информационных технологий Национального авиационного университета.
Kinzeryavyy Oleksiy, postgraduate student of Academic Department of IT-Security, National Aviation University.

Стокіпний Олександр Леонідович, кандидат технічних наук, доцент кафедри інформаційних систем факультету економічної інформатики, Харківського національного економічного університету ім. С. Кузнеця (ХНЕУ).
E-mail: a.stokipny@gmail.com
Стокипный Александр Леонидович, кандидат технических наук, доцент, доцент кафедры информационных систем факультета экономической информатики, Харьковского национального экономического университета им. С. Кузнеца (ХНЭУ).
Stokipnyy Oleksandr, Ph.D., docent of Academic Department of Information systems, Simon Kuznets Kharkiv National University of Economics.

УДК 004.056:007

МЕТОД ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ПІДТРИМКИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ СИСТЕМНОГО ПІДХОДУ

Дмитро Домарєв

Об'єднання розрізнених засобів захисту та зусиль фахівців різних профілів для виконання стратегічних завдань забезпечення інформаційної безпеки (ІБ) України потребує інформаційно-аналітичної підтримки управління ІБ на основі системного підходу. Відсутність узгодженої обробки та зберігання оперативних задач, знань та ризиків ІБ в умовах неповноти інформації, а також відсутність застосування системного підходу в процесі управління ІБ зменшує адаптивність та мобільність систем інформаційної безпеки. Вдосконалено модель логічних і функціональних зв'язків між складовими системи управління інформаційною безпекою (СУІБ), в якій за рахунок надання множині складових «напрямки» змінної розмірності забезпечено гнучкість процесів аналізу, прогнозування та інформаційно-аналітичної підтримки прийняття рішень щодо забезпечення ІБ. Вперше розроблено модель даних СУІБ, в якій за рахунок структуризації даних за моделлю логічних і функціональних зв'язків між складовими СУІБ забезпечено узгоджену обробку та зберігання оперативних задач, знань та ризиків ІБ в умовах неповноти інформації. Вперше розроблено метод інформаційно-аналітичної підтримки управління ІБ, який за рахунок використання вдосконаленої моделі зв'язків між складовими СУІБ, розробленої моделі даних СУІБ та розробленої методики оцінки поточного стану ІБ забезпечує застосування принципів системного підходу в управлінні ІБ. Наведено приклад застосування розробленого методу для банківської системи України. Надано рекомендації щодо наукового та практичного використання розроблених моделей та методу.

***Ключові слова**: системний підхід до інформаційної безпеки, модель зв'язків між складовими СУІБ, модель даних управління інформаційною безпекою, метод управління інформаційною безпекою, система управління інформаційною безпекою, СУІБ.*

Актуальність. Проблема управління інформаційною безпекою витікає з необхідності пошуку шляхів підвищення ефективності функціонування інформаційних систем (ІС) держави в сучасних умовах; оцінки ефективності побудови науково-методичного апарату та функціонування систем інформаційної безпеки (ІБ) України; розробки науково-методичних основ, технологій та засобів аналізу, прогнозування й інформаційно-аналітичної підтримки процесів прийняття рішень щодо забезпечення ІБ України; розробки методик та інструментарію оцінки стану ІБ як складової національної безпеки України.

До останнього часу контроль та управління системами ІБ відбувались фрагментарно та децентралізовано. Використовувались здебільшого вузько-направлені засоби захисту проти певних загроз, а відповідальними за них були різні особи. Це зменшує адаптивність та мобільність систем ІБ. Існує потреба об'єднати розрізнені засоби захисту та зусилля фахівців різних профілів ІБ в єдину систему управління інформаційною безпекою (СУІБ).

Проблемою займались зарубіжні та українські вчені, серед яких Бйорк Ф., Крішен Ж., Альбрехтсен Е., Калашніков А. О., Зирянова Т. Ю., Машкіна І. В., Зиков В. Д., Коваль З. В., Крапивенський А. С., Мєшков Є. П., Домарєв В. В., Юдін О. К., Корченко О. Г., Родіонов А. М., Іванченко Є. В., Чунарьова А. В., Гнатюк С. О., Казмірчук С. В. та інші.

Першою та досі найбільш вдалою спробою систематизувати управління ІБ була розробка системного підходу до ІБ [6].

В кінці 2010 р. з метою підвищення рівня інформаційної безпеки в банківській системі України Національний банк України (НБУ) запровадив два галузеві стандарти управління ІБ [4, 5], що фактично дублюють міжнародні стандарти «ISO/IEC 27001» та «ISO/IEC 27002», які визначають вимоги і правила впровадження СУІБ.

З початку 2013 р. урядом України ведеться розробка закону Про кібернетичну безпеку (на час публікації проект закону остаточно не прийнято).

В квітні-травні 2014 р. Рада національної безпеки і оборони України (РНБОУ) видала рішення Про заходи щодо вдосконалення державної політики у сфері ІБ та положення Про інформаційно-аналітичний центр, в яких поставлені різнорідні та стратегічні завдання забезпечення ІБ України, виконання яких потребує застосування системного підходу.

Викладене свідчить про потребу одночасно забезпечити гнучкість процесів аналізу, прогнозування та інформаційно-аналітичної підтримки управління ІБ, узгоджену обробку та зберігання оперативних задач, знань та ризиків ІБ в умовах неповноти інформації, оцінювання поточного стану ІБ на основі експертних оцінок, застосування принципів системного підходу в управлінні ІБ.

Перелічені факти обґрунтовують актуальність розробки моделей та методу інформаційно-аналітичної підтримки управління ІБ на основі системного підходу.

Зв'язок роботи з науковими та практичними завданнями. Виконання роботи безпосередньо витікає із задач, поставлених в:

– п. 4.3.8 Стратегії національної безпеки України, затвердженої Указами Президента України від 12.02.2007 р. № 105 та від 08.06.2012 р. № 389/2012;

– п. 4 рішення РНБОУ від 17.11.2010 р. Про виклики та загрози національній безпеці України у 2011 році, затвердженого Указом Президента України № 1119/2010 від 10.12.2010 р.;

– п. 3 положення Про інформаційно-аналітичний центр, затвердженого Указом Президента України № 398/2014 від 12.04.2014 р.;

– п. 1 рішення РНБОУ Про заходи щодо вдосконалення формування та реалізації державної політики у сфері ІБ України, затвердженого Указом Президента України № 449/2014 від 01.05.2014 р.

Мета дослідження. Метою роботи є розробка моделей та методу аналізу, прогнозування та інформаційно-аналітичної підтримки процесів прийняття рішень щодо управління ІБ на основі системного підходу, що дозволить оцінити ефективність побудови науково-методичного апарату та функціонування систем ІБ, систематизувати і об'єднати зусилля фахівців з ІБ різних профілів, оцінювати поточний стан ІБ.

Модель логічних і функціональних зв'язків між складовими СУІБ. Застосування системного підходу до ІБ спирається на модель логічних і функціональних зв'язків між складовими СУІБ [6] (так звану «Матрицю системного підходу до ІБ», рис. 1).

Відповідно до принципів системного підходу, складові СУІБ розділені на три множини (1): основи (з чого складається), напрямки (для чого призначено), етапи (як працює).

Класичні основи системного підходу до ІБ:

1. База (законодавча, нормативно-правова та наукова);

2. Структура (склад і завдання органів, підрозділів, що забезпечують ІБ);

3. Заходи (організаційно-технічні і режимні);

4. Засоби (програмно-технічні).

Класичні напрямки системного підходу до ІБ:

1. Захист об'єктів ІС;

2. Захист процесів, процедур і програм обробки інформації;

3. Захист каналів зв'язку;

4. Придушення побічних електромагнітних випромінювань;

5. Управління і контроль системи захисту.

Класичні етапи системного підходу до ІБ:

1. Визначення інформаційних і технічних ресурсів, а також об'єктів ІС, що підлягають захисту;

2. Виявлення множини потенційних загроз і каналів витоку інформації;

3. Оцінка вразливості і ризиків при наявній множині загроз і каналів витоку;

4. Формування вимог до СЗІ;

5. Обрання засобів захисту інформації та їх характеристик;

6. Впровадження і організація використання обраних заходів, способів і засобів захисту;

7. Контроль цілісності і управління захистом.

$$S = \{S_s\}, s \in [1;7];$$
$$D = \{D_d\}, d \in [1;5]; \quad (1)$$
$$B = \{B_b\}, b \in [1;4],$$

де S – множина етапів (stages), D – множина напрямків (directions), B – множина основ (bases).

Зв'язки між складовими СУІБ E_{sdb} представлені перетинами множин основ, етапів і напрямків та є частковими кількісними показниками відповідності заданому рівню ІБ (2). Наприклад, елемент E_{321} представляє «Нормативну базу проведення оцінки вразливостей в процесах і програмах ІС». E_{sdb} є нечіткими числами, функції належності яких визначаються на основі статистичних даних, експертних, або рангових оцінок.

$$E_{sdb} = S_s \bigcap D_d \bigcap B_b,$$
$$s \in [1;7], d \in [1;5], b \in [1;4], E_{sdb} \in [0;1]. \quad (2)$$

Множина зв'язків між складовими СУІБ M (3) утворює модель логічних і функціональних зв'язків між складовими СУІБ (так звану «Матрицю системного підходу до ІБ»), яка є множиною нечітких чисел. Графічно множину зв'язків зручно зображати у вигляді таблиці (рис. 1).

$$M = \{E_{sdb}\}, s \in [1;7], d \in [1;5], b \in [1;4]. \quad (3)$$

<<< Етапи	Напрямки >>>	010				020				030				040				050			
		Захист об'єктів ІС				Захист процесів і програм				Захист каналів зв'язку				ПЕМВН				Управління системою захисту			
	Основи >>>	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Визначення інформації, що підлягає захисту	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Виявлення загроз і каналів витоку інформації	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведення оцінки уразливості і ризиків	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Визначення вимог до СУІБ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Здійснення вибору засобів захисту	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Впровадження і використання обраних заходів і засобів	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль цілісності і управління захистом	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Рис. 1. Представлення класичної множини зв'язків між складовими СУІБ у вигляді таблиці

Кардинальне число (потужність) нечіткої множини – характеристика, що узагальнює поняття кількості її елементів (4).

$$cardA = |A| = \sum_{i=1}^{n} \mu^A(x_i), \quad (4)$$

де A – нечітка множина, $\mu^A(x)$ – функція належності елемента x до множини A.

Кардинальне число може бути використане в оцінці загального рівня ІБ.

За інформацією, отриманою під час впровадження системного підходу до ІБ, з розвитком ІТ з'являються нові напрямки ІБ а деякі з існуючих (наприклад, придушення побічних електромагнітних випромінювань) втрачають актуальність. При цьому набори основ та етапів ІБ залишаються незмінними. Якщо напрямки ІБ не відповідають дійсності, відповідні елементи мають малі ступені належності до загального рівня ІБ, що в

свою чергу знижує точність оцінки загального рівня ІБ. Це призводить до зменшення спостережуваності та керованості СУІБ.

Для забезпечення гнучкості процесів аналізу, прогнозування та інформаційно-аналітичної підтримки прийняття рішень щодо забезпечення ІБ, та для застосування системного підходу в управлінні ІБ, множині напрямків надано змінну розмірність без обов'язкових значень, щоб їх можна було визначати в залежності від специфіки цільової організації.

Основу № 3 «Заходи» перейменовано у «Політика», оскільки цей термін доцільніший з точки зору управління ІБ. Визначення етапів № 1, 4, 6, 7 також конкретизовані відносно управління ІБ.

Вдосконалені основи системного підходу до ІБ:

1. База (законодавча, нормативно-правова та наукова);
2. Структура (склад і завдання органів, підрозділів, що забезпечують ІБ);
3. Політика ІБ;
4. Засоби (програмно-технічні).

Вдосконалені напрямки системного підходу до ІБ визначаються в залежності від специфіки цільової організації.

Вдосконалені етапи системного підходу до ІБ:

1. Визначення активів, що підлягають захисту;
2. Виявлення множини потенційних загроз і каналів витоку інформації;
3. Оцінка вразливості і ризиків при наявній множині загроз і каналів витоку;
4. Формування вимог до СУІБ;
5. Обрання засобів захисту інформації та їх характеристик;
6. Впровадження, навчання та використання СУІБ;
7. Контроль та оцінка ефективності СУІБ.

Вдосконалену модель описує вираз (5).

$$M = \{E_{sdb}\},\ E_{sdb} = S_s \bigcap D_d \bigcap B_b,$$
$$s \in [1;7], d \in [1;k], b \in [1;4],\ E_{sdb} \in [0;1]. \quad (5)$$

де M – множина зв'язків між складовими СУІБ, E_{sdb} – зв'язки між складовими СУІБ, S – множина етапів, D – множина напрямків, B – множина основ, k – кількість елементів множини напрямків.

Оскільки множина напрямків змінна, модель адаптується до конкретних галузей, ситуацій, задач. Визначено напрямки та наведено приклад моделі зв'язків між складовими СУІБ банківських установ (рис. 2). Для даної галузі визначені наступні напрямки: система електронних платежів НБУ, карткові платіжні системи, інформаційні системи банку, системи електронної комерції, комунікації.

<<< Етапи	Напрямки >>>	010				020				030				040				050			
		Система електронних платежів НБУ				Карткові платіжні системи				Інформаційні системи банку (АБС)				Системи електронної комерції				Комунікації			
	Основи >>>	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Визначення активів, що підлягають захисту	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Виявлення загроз і каналів витоку	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Оцінка ризиків	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Формування вимог до СУІБ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Визначення засобів та заходів ІБ	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Впровадження, навчання та використання СУІБ	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль та оцінка ефективності СУІБ	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Рис. 2. Вдосконалена модель зв'язків між складовими СУІБ. Приклад для банківських установ

Модель даних СУІБ. Для впорядкування та обробки даних згідно з принципами системного підходу до ІБ була створена спеціальна модель даних СУІБ.

В розробленій моделі даних є три множини об'єктів (знання, задачі, ризики) та множина елементів класифікації. Останні призначені для впорядкування документів та задач згідно з розробленою моделлю зв'язків між складовими СУІБ.

В розробленій моделі даних запропоновано наступний набір елементів класифікації: Напрямки, Об'єкти, Співробітники, Документи, Заходи, Засоби, Етапи, Активи, Загрози, Вимоги, Вирішення, Впровадження, Контроль.

Відповідно до зазначеного переліку, множина елементів класифікації (6) складається з 13-ти підмножин, які є власне елементами класифікації і містять переліки значень (7). Розроблена модель

даних призначена для управління ІБ в умовах неповноти інформації, тому підмножини мають необмежену перемінну розмірність.

$$C = \{C^i\}, i \in [1;13], \tag{6}$$

$$C^1 = \{c^1_a\}, a \in [1;a']; C^2 = \{c^2_b\}, b \in [1;b']; \\ \dots\ C^{13} = \{c^{13}_m\}, m \in [1;m'], \tag{7}$$

де C – множина елементів класифікації, C^i – елементи класифікації, c^i_k – значення елементів, a', b', … m' – кількості значень елементів у відповідних підмножинах.

Елементи даних типу «Знання» містять інформацію про вхідні нормативні документи і аналітичні дані. Елемент знання складається з даних, що описують власне розділ документа (заголовок, опис, зміст, посилання і т. п.) та елементів класифікації (8). В елементі знання можуть бути представлені не всі елементи класифікації, але не менше одного, щоб елемент знання обов'язково мав місце в моделі зв'язків між складовими СУІБ.

$$K = \{K_i\}, K_i = \{k_i, c^1_a, \dots, c^j_x\}, \\ i \in [1;n], j \in [1;13], \tag{8}$$

де K – множина елементів типу «Знання», K_i – елемент знання, k_i – дані, що описують розділ документа, c^j_x – значення елементів класифікації, n – кількість елементів типу «Знання».

Елементи даних типу «Задачі» містять інформацію про оперативні задачі. Елемент задач складається з даних, що описують власне задачу (строки виконання, керівник, відповідальний, виконавці, постановка задачі, стан виконання і т. п.) та елементів класифікації (9). В елементі задач можуть бути представлені не всі елементи класифікації, але не менше одного, щоб елемент задач обов'язково мав місце в моделі зв'язків між складовими СУІБ.

$$T = \{T_i\}, T_i = \{t_i, c^1_a, \dots, c^j_x\}, \\ i \in [1;m], j \in [1;13], \tag{9}$$

де T – множина елементів типу «Задачі», T_i – елемент задач, t_i – дані, що описують власне задачу, c^j_x – значення елементів класифікації, m – кількість елементів типу «Задачі».

Елементи даних типу «Ризик» визначено як пари «актив-загроза» (10).

$$R = \{R_i\}, R_i = \{c^8_j, c^9_k\}, i \in [1;l], \tag{10}$$

де R – множина елементів типу «Ризики», R_i – елемент ризиків, c^8_j – значення елемента класифікації «Активи», c^9_k – значення елемента класифікації «Загрози», l – кількість елементів типу «Ризики».

Враховуючи (6)-(10), розроблену модель даних описує кортеж (11).

$$\langle C, K, T, R \rangle = \langle \{C^i\}, \{K_i\}, \{T_i\}, \{R_i\} \rangle. \tag{11}$$

Розроблена модель даних відповідає поставленій меті дослідження, оскільки відповідає принципам системного підходу до ІБ [6] та забезпечує можливості аналізу, прогнозування та інформаційно-аналітичної підтримки процесів прийняття рішень щодо управління ІБ.

Метод інформаційно-аналітичної підтримки управління ІБ. Вперше розроблено метод інформаційно-аналітичної підтримки управління ІБ на основі системного підходу, (рис. 3) який за рахунок використання вдосконаленої моделі зв'язків між складовими СУІБ, розроблених автором моделі даних СУІБ та методики оцінки поточного стану ІБ [2] забезпечує застосування принципів системного підходу в управлінні ІБ.

Розроблений метод спирається на головні принципи системного підходу: системної погодженості, процедурної повноти, функціональної ортогональності, інформаційної взаємозалежності, цілеспрямованої відповідності, функціональної раціональності, багатоцільової загальності, багатофакторної адаптивності, процедурної відкритості, раціональної доповнюваності [9].

Вхідними даними для методу є складові СУІБ $C = \{C^i\}$ (6), нормативні документи і аналітичні дані $K = \{K_i\}$ (8), оперативні задачі $T = \{T_i\}$ (9), методи оцінювання імовірностей переходів системи між визначеними станами.

Вихідними даними методу є політика ІБ, впорядковані і узгоджені оперативні задачі $T = \{T_i\}$, $T_i = \{t_i, c^1_a, \dots, c^j_x\}$ (9), оцінка загального рівня вразливості ІС $\sum V_a$, найбільш вразливі активи $V_a = \sum R_a$, найбільш небезпечні загрози N_k, пріоритети в усуненні вразливостей ІБ, поточний стан СУІБ.

Модель зв'язків між складовими СУІБ забезпечує встановлення, систематизацію, аналіз та оцінювання взаємодії складових СУІБ.

Модель даних СУІБ забезпечує узгоджену обробку та зберігання визначених зв'язків між складовими СУІБ (5), елементів класифікації (7), знань (8), оперативних задач (9) та ризиків ІБ (10).

Методика оцінки поточного стану ІБ на основі експертних оцінок ризиків [2] забезпечує визначення загального рівня вразливості ІС, списків найбільш вразливих активів та найбільш небезпечних загроз, пріоритетів в усуненні вразливостей ІБ.

Модель стану СУІБ на основі напівмарківського процесу, розроблена автором та описана у [7, 8, 10], забезпечує аналіз та прогнозування стану СУІБ, спираючись на вхідні методи оцінювання імовірностей переходів, знання $K = \{K_n\}$ та інформацію щодо оперативних задач $T = \{T_m\}$, загроз $C^9 = \{c^9{}_k\}$ і N_k, рівня вразливості ІС $\sum V_a$.

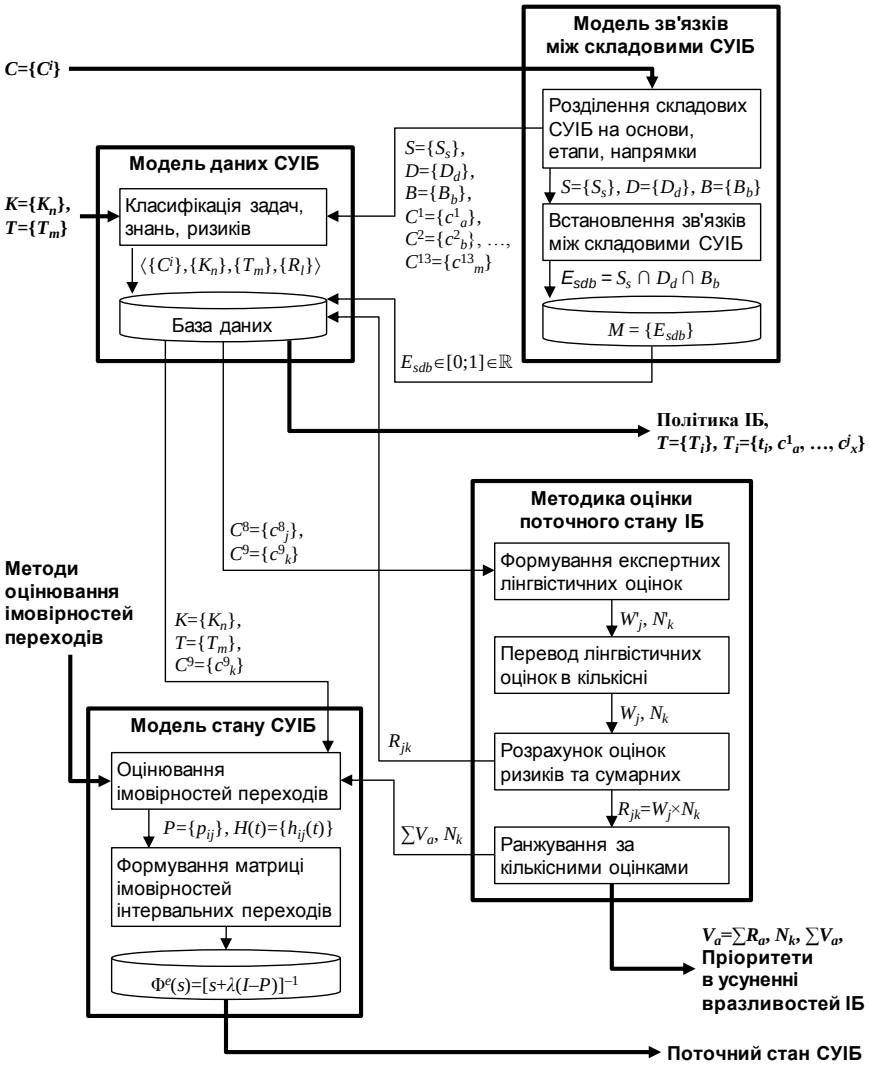


Рис. 3. Схема функціонування методу інформаційно-аналітичної підтримки управління ІБ на основі системного підходу

Основні **принципи** розробленого методу є:

1. Головна мета системи інформаційної безпеки – забезпечення потрібного (заданого) рівня ІБ;

2. Встановлення логічних і функціональних системних зв'язків між усіма елементами системи ІБ (процесами, організаційними, нормативно-методичними та технічними компонентами);

3. Первинне значення мають ті властивості елементів, які визначають міру їх взаємодії і чинять вплив на систему в цілому, а значущість властивостей окремих елементів знижується;

4. Систематизація елементів ІБ за групами складових моделі ІБ: основами (з чого складається), напрямками (для чого призначена) та етапами (як працює);

5. Поєднання знань, задач та нормативних документів в єдину систему.

Приклади застосування розробленого методу в банківських установах описано в [1, 3].

Приклад застосування розробленого методу для банківської системи України. Робота методу є реакцією на зміни вхідних даних, або на їх подання (в разі початку застосування методу). Для даного прикладу застосовані типові вхідні дані для банківських установ [1]:

1. Складові СУІБ (6)-(7):

1.1. Напрямки: система електронних платежів (СЕП) НБУ, карткові платежі, електронні платежі, документообіг, комунікації, …

1.2. Об'єкти: комп'ютерна мережа банку, ІС банку, електронні платіжні системи, карткові платіжні системи, об'єкти СУІБ банку, …

1.3. Співробітники: керівництво банку, відділ кадрів, юридичний підрозділ, підрозділ ІБ, підрозділ інформаційних технологій, …

1.4. Документи: закони України, документи НБУ, міжнародні документи, документи верхнього рівня, документи нижнього рівня, …

1.5. Заходи: оцінка та оброблення ризиків, координація ІБ, процедури контролю змін, управління технічною вразливістю, контроль доступу до мережі , …

1.6. Засоби: засоби безпеки ІС, засоби резервного копіювання, криптографічні засоби, системи безперебійного живлення, системи контролю доступу, …

1.7. Етапи: аналіз ресурсів СУІБ, оцінка ризиків, визначення політики, впровадження та функціонування, моніторинг та перегляд, …

1.8. Активи: активи СЕП НБУ, електронний документообіг, інфраструктура ІС, операційні системи, прикладні програми користувачів, …

1.9. Загрози: загрози комп'ютерній мережі, загрози СЕП НБУ, інсайдери, промисловий шпіонаж, фізичне пошкодження, …

1.10. Вимоги: перегляд політики ІБ, розподіл відповідальності, незалежний перегляд ІБ, контроль підключень до мережі, контроль технічних вразливостей, …

1.11. Вирішення: застосування контролів, прийняття ризиків, уникнення ризиків, перенесення ризиків, обмеження доступу, …

1.12. Впровадження: функціонування СУІБ, підвищення кваліфікації, налаштування обладнання, навчання персоналу, конференції, семінари, …

1.13. Контроль: зовнішній аудит, внутрішній аудит, контроль ІС банку, контроль персоналу, контроль фізичного середовища, …

2. Оперативні задачі з виконання поточної діяльності, вимог нормативних документів, заходів ІБ;

3. Нормативні документи і аналітичні дані щодо банківської діяльності;

4. Методи оцінювання імовірностей переходів для моделі стану СУІБ: системний аналіз, нечітка логіка, експертне оцінювання.

Модель зв'язків між складовими СУІБ отримує в якості вхідних даних складові СУІБ. Розділення їх на основи, етапи і напрямки відбувається експертними методами та методами системного аналізу. Далі формується множина зв'язків між складовими СУІБ (5).

Вихідними даними моделі зв'язків між складовими СУІБ є:

1. Множина зв'язків між складовими СУІБ банківських установ (рис. 4).

2. Основи: база (законодавча, нормативно-правова та наукова); структура (склад і завдання органів, підрозділів, що забезпечують ІБ); політика ІБ; засоби (програмно-технічні).

3. Етапи: визначення активів, що підлягають захисту; виявлення множини потенційних загроз і каналів витоку інформації; оцінка вразливості і ризиків при наявній множині загроз і каналів витоку; формування вимог до СУІБ; обрання засобів захисту інформації та їх характеристик; впровадження, навчання та використання СУІБ; контроль та оцінка ефективності СУІБ.

4. Напрямки: система електронних платежів НБУ; карткові платіжні системи; інформаційні системи банку; системи електронної комерції; комунікації.

5. Складові СУІБ, упорядковані згідно (7).

Всі вихідні дані передаються до моделі даних СУІБ.

<<< Етапи	Напрямки >>>	010				020				030				040				050			
		Система електронних платежів НБУ				Карткові платіжні системи				Інформаційні системи банку (АБС)				Системи електронної комерції				Комунікації			
	Основи >>>	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Визначення активів, що підлягають захисту	0,21	0,78	0,12	0,20	0,41	0,91	0,53	0,60	0,30	0,20	0,20	0,34	0,59	0,54	0,84	0,18	0,98	0,00	0,81	0,14
200	Виявлення загроз і каналів витоку	0,60	0,05	0,52	0,16	1,00	0,59	0,56	0,80	0,80	1,00	0,99	0,90	0,13	0,91	0,58	0,97	0,10	0,61	0,97	0,34
300	Оцінка ризиків	0,41	0,37	0,93	1,00	0,83	0,91	0,80	0,49	0,41	0,50	0,35	0,75	0,64	1,00	1,00	0,43	0,56	1,00	0,54	0,30
400	Формування вимог до СУІБ	0,04	0,64	0,34	0,64	0,03	1,00	1,00	1,00	0,06	0,11	0,43	0,83	0,78	0,90	0,23	0,94	0,84	0,92	0,37	0,10
500	Визначення засобів та заходів ІБ	0,49	0,30	0,59	0,64	0,75	0,38	0,46	0,24	0,37	0,65	0,72	0,42	0,66	0,07	0,06	0,72	0,37	0,32	0,53	0,67
600	Впровадження, навчання та використання СУІБ	0,13	0,39	1,00	0,20	0,76	0,71	0,83	0,62	1,00	0,54	0,51	0,38	1,00	0,72	0,73	0,08	0,16	0,11	0,16	0,32
700	Контроль та оцінка ефективності СУІБ	0,80	0,17	0,26	0,07	0,31	0,90	0,95	0,63	0,30	0,48	0,06	0,27	0,68	0,68	0,27	1,00	0,67	0,18	0,84	0,05

Рис. 4. Сформована множина зв'язків між складовими СУІБ банківських установ

Модель даних СУІБ отримує в якості вхідних даних оперативні задачі, нормативні документи і аналітичні дані, а також від моделі зв'язків між складовими СУІБ – множину зв'язків між

складовими СУІБ, основи, етапи, напрямки та упорядковані складові СУІБ.

Відбувається класифікація задач, знань і ризиків експертними методами згідно (8)-(10), результати якої (11) зберігаються в базі даних. Приклади представлення елементів задач та знань в базі даних представлено на рис. 5 та рис. 6 відповідно.

Створення політики ІБ верхнього рівня відбувається шляхом групування усіх наявних знань за напрямами ІБ цільової організації, потім за загрозами, характерними для кожного з напрямів, а потім – за заходами, націленими на протидію цим загрозам.

Вихідні дані моделі даних СУІБ є наступними:

1. Політика ІБ верхнього рівня (рис. 7);
2. Оперативні задачі (9), нормативні документи та аналітичні дані (8), перелік загроз – передаються до моделі стану СУІБ;
3. Переліки загроз та активів – передаються до методики оцінки поточного стану ІБ.

В якості зворотного зв'язку від методики оцінки поточного стану ІБ до моделі даних СУІБ надходить перелік ризиків (табл. 1). Оперативні задачі також є вихідними даними розробленого методу.

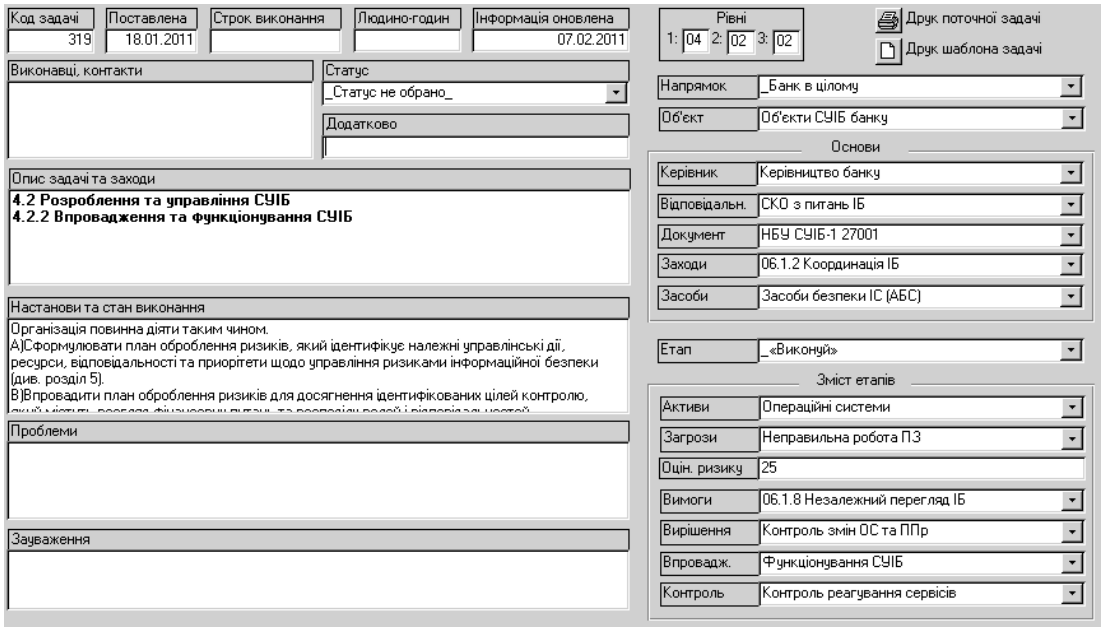


Рис. 5. Приклад представлення елемента задач в базі даних

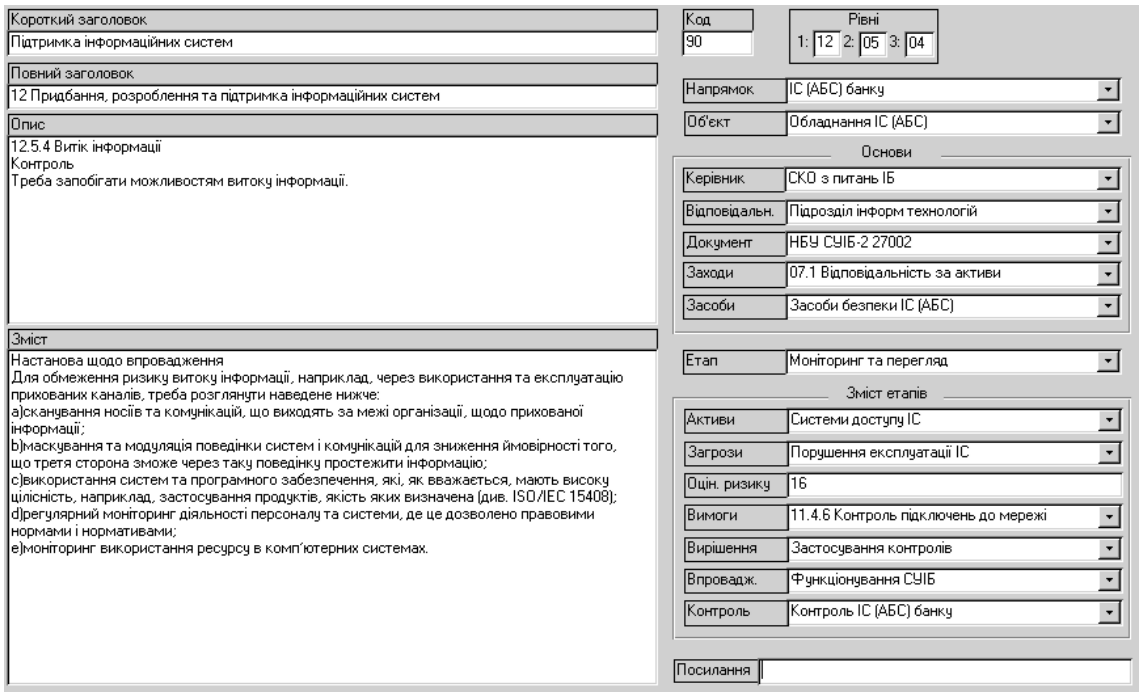
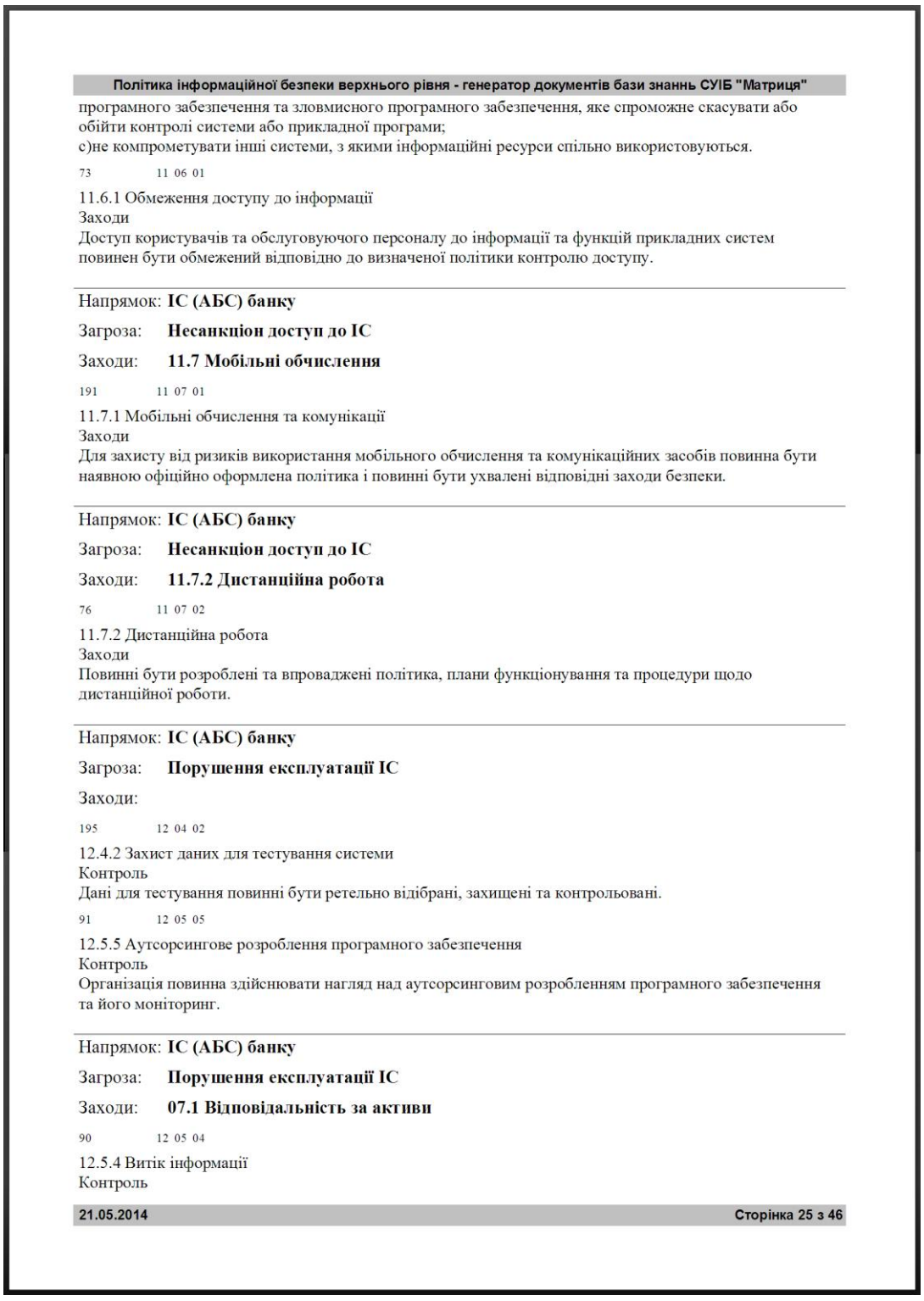


Рис. 6. Приклад представлення елемента знань в базі даних



Політика інформаційної безпеки верхнього рівня - генератор документів бази знанньь СУІБ "Матриця"

програмного забезпечення та зловмисного програмного забезпечення, яке спроможне скасувати або обійти контролі системи або прикладної програми;
с)не компрометувати інші системи, з якими інформаційні ресурси спільно використовуються.

73 11 06 01

11.6.1 Обмеження доступу до інформації
Заходи
Доступ користувачів та обслуговуючого персоналу до інформації та функцій прикладних систем повинен бути обмежений відповідно до визначеної політики контролю доступу.

Напрямок: **ІС (АБС) банку**

Загроза: **Несанкціон доступ до ІС**

Заходи: **11.7 Мобільні обчислення**

191 11 07 01

11.7.1 Мобільні обчислення та комунікації
Заходи
Для захисту від ризиків використання мобільного обчислення та комунікаційних засобів повинна бути наявною офіційно оформлена політика і повинні бути ухвалені відповідні заходи безпеки.

Напрямок: **ІС (АБС) банку**

Загроза: **Несанкціон доступ до ІС**

Заходи: **11.7.2 Дистанційна робота**

76 11 07 02

11.7.2 Дистанційна робота
Заходи
Повинні бути розроблені та впроваджені політика, плани функціонування та процедури щодо дистанційної роботи.

Напрямок: **ІС (АБС) банку**

Загроза: **Порушення експлуатації ІС**

Заходи:

195 12 04 02

12.4.2 Захист даних для тестування системи
Контроль
Дані для тестування повинні бути ретельно відібрані, захищені та контрольовані.

91 12 05 05

12.5.5 Аутсорсингове розроблення програмного забезпечення
Контроль
Організація повинна здійснювати нагляд над аутсорсинговим розробленням програмного забезпечення та його моніторинг.

Напрямок: **ІС (АБС) банку**

Загроза: **Порушення експлуатації ІС**

Заходи: **07.1 Відповідальність за активи**

90 12 05 04

12.5.4 Витік інформації
Контроль

21.05.2014 **Сторінка 25 з 46**

Рис. 7. Витяг зі сформованої політики ІБ верхнього рівня

Методика оцінки поточного стану ІБ отримує в якості вхідних даних від моделі даних СУІБ переліки загроз та активів.

Принцип функціонування методики викладений в [2]. Для даного прикладу вихідними даними методики оцінки поточного стану ІБ будуть:

1. Перелік ризиків ІБ та їх оцінок (табл. 1) – передається до моделі даних СУІБ;

2. Перелік найбільш небезпечних загроз (рис. 8) та пріоритети в усуненні вразливостей ІБ (перелік найбільш вразливих активів, рис. 9) – передаються до моделі стану СУІБ;

3. Оцінка загального рівня захищеності ІС – 321 бал.

Перелік найбільш небезпечних загроз та пріоритети в усуненні вразливостей ІБ (перелік найбільш вразливих активів) також є вихідними даними розробленого методу.

Таблиця 1

Сформований перелік ризиків ІБ та їх оцінок

Загроза	Частота	Актив	Збиток	Оцінка ризику
Загрози комп'ютерній мережі	5	Активи СЕП НБУ	5	25
Загрози СЕП НБУ	3	Інфраструктура ІС (АБС)	5	15
Інсайдери	4	Активи СЕП НБУ	5	20
Інсайдери	4	Ел. документообіг	3	12
Промисловий шпіонаж	5	Ел. документообіг	3	15
Фізичне пошкодження	2	Активи СЕП НБУ	5	10
«Чорна пошта»	1	Ел. документообіг	3	3
Ввід фальсифікованих даних	4	Ел. документообіг	3	12
Віддалений шпіонаж	1	Ел. документообіг	3	3
Віруси	4	Активи СЕП НБУ	5	20
Віруси	4	Ел. документообіг	3	12
Втрата доступності	4	Активи СЕП НБУ	5	20
Втрата доступності	4	Ел. документообіг	3	12
Втрата конфіденційності	3	Активи СЕП НБУ	5	15
Втрата конфіденційності	3	Ел. документообіг	3	9
Втрата конфіденційності	3	Системи доступу ІС	4	12
Втрата цілісності	5	Активи СЕП НБУ	5	25
Втрата цілісності	5	Ел. документообіг	3	15
Неправильна робота ПЗ	5	Операційні системи	5	25
Пожежа	5	Активи СЕП НБУ	5	25
Порушення експлуатації ІС	4	Системи доступу ІС	4	16

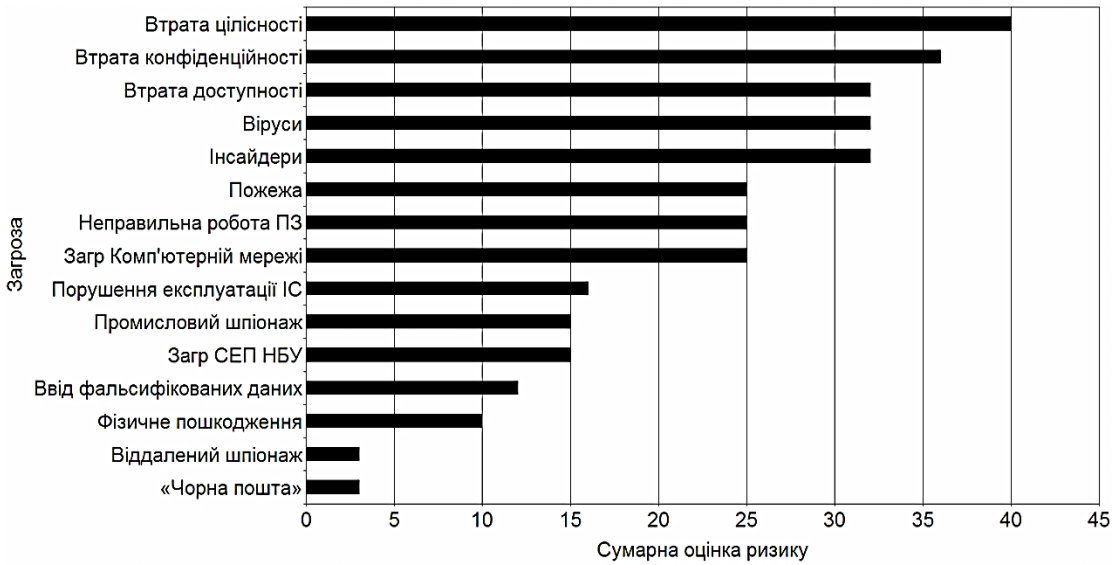


Рис. 8. Представлення найбільш небезпечних загроз

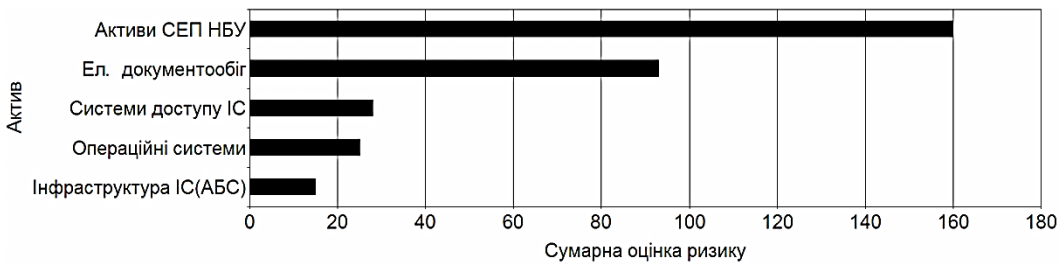


Рис. 9. Представлення найбільш вразливих активів

Модель стану СУІБ отримує в якості вхідних даних методи оцінювання імовірностей переходів; від моделі даних СУІБ – оперативні задачі, нормативні документи, аналітичні дані, перелік загроз; від методики оцінки поточного стану ІБ – переліки найбільш небезпечних загроз та найбільш вразливих активів.

Принцип функціонування моделі викладений в [7, 8, 10]. Для даного прикладу вихідними даними моделі стану СУІБ буде поточний стан СУІБ – «Захист» (успішна протидія загрозам).

Отже, **для даного прикладу отримані наступні вихідні дані методу:**

1. Політика ІБ верхнього рівня (рис. 7);
2. Впорядковані і узгоджені оперативні задачі (рис. 5);
3. Оцінка загального рівня вразливості ІС – 321 бал;
4. Пріоритети в усуненні вразливостей ІБ (перелік найбільш вразливих активів, рис. 9)
5. Перелік найбільш небезпечних загроз (рис. 8);
6. Поточний стан СУІБ – «Захист» (успішна протидія загрозам).

Висновки:

1. Вдосконалено модель логічних і функціональних зв'язків між складовими СУІБ, в якій за рахунок надання множині складових «напрямки» змінної розмірності забезпечено гнучкість процесів аналізу, прогнозування та інформаційно-аналітичної підтримки прийняття рішень щодо забезпечення ІБ.

2. Вперше розроблено модель даних СУІБ, в якій за рахунок структуризації даних за моделлю логічних і функціональних зв'язків між складовими СУІБ забезпечено узгоджену обробку та зберігання оперативних задач, знань та ризиків ІБ в умовах неповноти інформації.

3. Вперше розроблено метод інформаційно-аналітичної підтримки управління ІБ, який за рахунок використання вдосконаленої моделі зв'язків між складовими СУІБ, розробленої моделі даних СУІБ та розробленої методики оцінки поточного стану ІБ забезпечує застосування принципів системного підходу в управлінні ІБ.

4. Наукове та практичне використання розроблених моделей та методу управління ІБ можливе в:

4.1. Оцінці ефективності побудови науково-методичного апарату та функціонування системи ІБ України та її основних елементів;

4.2. Аналітичному та прогнозному супроводженні діяльності РНБОУ з питань національної безпеки в інформаційній сфері;

4.3. Розробці законів та інших нормативних документів з ІБ, наприклад закону України Про кібернетичну безпеку, Доктрини інформаційної безпеки України;

4.4. Організації інформаційно-методичного ядра змісту викладання предметів спеціальностей «інформаційна безпека», «захист інформації» і т.п.

ЛІТЕРАТУРА

[1]. Домарєв В.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) [Текст] / В.В. Домарєв, Д.В. Домарєв. – Донецьк: «Велстар», 2012. – 146 с. – ISBN 978-966-2759-00-6.

[2]. Домарєв Д.В. Методика оцінювання захищеності інформаційних систем за допомогою СУІБ «Матриця» [Текст] / Д.В. Домарєв, В.В. Домарєв, С.Д. Прокопенко // Захист інформації – К.: НАУ, 2013. – Том 15, № 1. – С. 80 – 86. – ISSN 2221-5212

[3]. Домарєв Д.В. Методика управління інформаційною безпекою в банківських установах за допомогою СУІБ «Матриця» [Текст] / Д.В. Домарєв, В.В. Домарєв // Безпека інформації – К.: Наш формат, 2013. – Том 19, № 1. – С. 60 – 70. – ISSN 2225-5036

[4]. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD) [Текст]: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – К.: Національний банк України, 2010. – 49 с. – Код УКНД 35.040.

[5]. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [Текст]: ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – К.: Національний банк України, 2010. – 163 с. – Код УКНД 35.040.

[6]. Домарев В.В. Безопасность информационных технологий. Системный подход [Текст] / В.В. Домарев. – К.: ООО «ТИД «ДС», 2004. – 992 с. – ISBN 966-7992-36-5

[7]. Домарев Д.В. Применение полумарковских процессов в разработке и описании состояния систем защиты информации [Текст] / Д.В. Домарев // Системи обробки інформації: Зб. наук. пр. – Х.: ФОП «Азамаєва В.П.», 2009. – Вип. 7(79). – С. 19 – 24. – ISSN 1681-7710

[8]. Домарев Д.В. Математическое описание процессов атак на компьютерные сети [Текст] / Д.В. Домарев // Проблеми інформатизації та управління: Зб. наук. пр. – К.: НАУ, 2010. – Вип. 1(29). – С. 50 – 54. – ISSN 2073-4751

[9]. Згуровский М.З. Системный анализ: проблемы, методология, приложения [Текст] / М.З. Згуровский, Н.Д. Панкратова; Ин-т прикладного системного анализа НАН Украины. – К.: Наукова думка, 2011. – 726 с. – ISBN 978-966-00-1124-3.

[10]. Domarev D.V. Application of semi-Markov processes for heterogeneous computer networks modeling

[Текст] / D.V. Domarev // IX Міжнародна наукова конференція студентів та молодих учених «Політ»: Зб. тез. – К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2009. – С. 267.

REFERENCES

[1]. Domarev V.V. *Upravlinnya informatsiynoyu bezpekoyu v bankivskykh ustanovakh (Teoriya i praktyka vprovadzhennya standartiv seriyi ISO 27k)* [Information security management in banking institutions (Theory and practice of ISO 27k standards implementation)]. Donetsk: «Welstar», 2012. 146 p.

[2]. Domarev D.V., Domarev V.V., Prokopenko S.D. Method of information system's security level estimation using ISMS "Matrix". *Zakhyst infotmatsiyi*. 2013; 1(15): p. 80-86.

[3]. Domarev D.V., Domarev V.V. Method of information security management in banking institutions using ISMS "Matrix". Bezpeka informatsiyi. 2013; 1(19): p. 60-70.

[4]. *Informatsiyni tekhnologiyi. Metody zakhystu. Systema upravlinnya informatsiynoyu bezpekoyu (ISO/IEC 27001:2005, MOD): GSTU SUIB 1.0/ISO/IEC 27001:2010* [Information technology – Security techniques – Information security management system (ISO/IEC 27001:2005, MOD): Branch standard of Ukraine ISMS 1.0/ISO/IEC 27002:2010]. Kyyiv: National bank of Ukraine, 2010. 49 p.

[5]. *Informatsiyni tekhnologiyi. Metody zakhystu. Zvid pravyl dlya upravlinnya informatsiynoyu bezpekoyu (ISO/IEC 27002:2005, MOD): GSTU SUIB 2.0/ISO/IEC 27002:2010* [Information technology – Security techniques – Code of practice for information security management (ISO/IEC 27002:2005, MOD): Branch standard of Ukraine ISMS 2.0/ISO/IEC 27002:2010]. Kyiv: National bank of Ukraine, 2010. 163 p.

[6]. Domarev V.V. *Bezopasnost ynformatsyonnykh tekhnologyy. Systemnyy podkhod* [IT security. The system approach]. Kyyiv: OOO "TID DS", 2004. 992 p.

[7]. Domarev D.V. Application of semi-Markov processes in design and state description of information security systems. *Systemy obrobky informatsiyi*. 2009; 7(79): p. 19-24.

[8]. Domarev D.V. Mathematical description of computer network attacking processes. *Problemy informatyzatsiyi ta upravlinnya*. 2010; 1(29): p. 50-54.

[9]. Zgurovskyy M.Z., Pankratova N.D. *Systemnyy analiz: problemy, metodologiya, prilozheniya* [System analysis: problems, methodology, applications]. Kyyiv: "Naukova dumka", 2011. 726 p.

[10]. Domarev D.V. Application of semi-Markov processes for heterogeneous computer networks modelling. *IX Mizhnarodna naukova konferentsiya studentiv ta molodykh uchenykh "Polit" (IX International scientific conference of students and young scientists "Polit")*. Kyyiv: "Naudruk", 2009, p. 267.

МЕТОД ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ПОДДЕРЖКИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ СИСТЕМНОГО ПОДХОДА

Объединение разнородных средств защиты и усилий специалистов разных профилей для выполнения стратегических заданий обеспечения информационной безопасности (ИБ) Украины требует информационно-аналитической поддержки управления ИБ на основе системного подхода. Отсутствие согласованной обработки и хранения оперативных задач, знаний и рисков ИБ в условиях неполноты информации, а также отсутствие применения системного подхода в процессе управления ИБ уменьшает адаптивность и мобильность систем информационной безопасности. Усовершенствована модель логических и функциональных связей между составляющими системы управления информационной безопасностью (СУИБ), в которой за счет назначения множеству составляющих «направления» переменной размерности обеспечена гибкость процессов анализа, прогнозирования и информационно-аналитической поддержки принятия решений по обеспечению ИБ. Впервые разработана модель данных СУИБ, которая за счет структуризации данных в соответствии с моделью логических и функциональных связей между составляющими СУИБ обеспечивает согласованную обработку и хранение оперативных задач, знаний и рисков ИБ в условиях неполноты информации. Впервые разработан метод информационно-аналитической поддержки управления ИБ, который за счет использования усовершенствованной модели связей между составляющими СУИБ, разработанной модели данных СУИБ и разработанной методики оценки текущего состояния ИБ обеспечивает применение принципов системного подхода в управлении ИБ. Приведен пример использования разработанного метода для банковской системы Украины. Предоставлены рекомендации по научному и практическому применению разработанных моделей и метода.

Ключевые слова: системный подход к информационной безопасности, модель связей между составляющими СУИБ, модель данных управления информационной безопасностью, метод управления информационной безопасностью, система управления информационной безопасностью, СУИБ.

METHOD OF INFORMATION& ANALYTICAL SUPPORT OF INFORMATION SECURITY MANAGEMENT BASED ON THE SYSTEM APPROACH

Informative-analytical support of information security management based on the system approach is used to unite the heterogeneous security means and the forces of different security specialists in order to fulfil the strategic tasks of Ukraine's national information security. The model of logical and functional relations between the

components of an information security management system (ISMS) is improved. The set of components named "Directions" is given a variable length. This provides the flexibility to the processes of analysis, prognostication and informative-analytical support for the decisions concerning information security. For the first time the information security management system data model is developed, that provides concerted processing and storage of operational tasks, knowledge and information security risks under the incompleteness of information. The data is structured according to the improved model of logical and functional relations between the components of an ISMS. For the first time the method of informative-analytical support for information security management is developed, which provides the system approach principles application in information security management. The method is based on the improved model of relations between the components of an ISMS, the developed information security management data model and the developed technique of current information security state estimation. An example of the developed method application in Ukraine's banking system is presented. Recommendations for the scientific and practical use of the developed models and method are provided.
Keywords: system approach to information security, model of relations between the components of an ISMS, data model for information security management, information security management method, information security management system, ISMS.

Домарєв Дмитро Валерійович, аспірант, Національний авіаційний університет.
E-mail: dimavsesvit@yahoo.com.
Домарев Дмитрий Валериевич, аспирант, Национальный авиационный університет.
Domarev Dmitry, postgraduate student of the National aviation university.

УДК 004.056.57

СТАТИСТИЧЕСКИЕ СВОЙСТВА ТРАФИКА НА ОСНОВЕ BDS-ТЕСТОВ ДЛЯ РЕАЛИЗАЦИИ СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

Алексей Смирнов, Юрий Дрейс, Дмитрий Даниленко

В работе предлагается использовать математический аппарат статистического анализа на основе BDS-тестов для исследования свойств сетевого трафика различных служб и информационных сервисов при определении значимости расхождения или совпадения их характеристик. Полученные результаты экспериментальных исследований статистических свойств сетевого трафика с использованием корреляционного анализа временных рядов подтверждают теоретические предположения о том, что для различных видов трафика (HTTP, FTP, Skype трафик и потоковое вещание) результат BDS-теста дает различные значения, которые могут быть приняты в качестве эталонных при использовании и усовершенствовании механизмов мониторинга сетевой активности, в том числе и для реализации системы обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях.
Ключевые слова: *телекоммуникационные системы и сети, система обнаружения и предотвращения вторжений, BDS-статистика, статистические свойства трафика.*

Введение. Современное развитие телекоммуникационных систем и сетей и применяемых компьютерных технологий привело к появлению качественно новых услуг и сервисов в информационной сфере, внедрению передовых технологий обработки и передачи данных и их доступности широкой пользовательской аудитории [1]. В тоже время интенсивное развитие современных компьютерных технологий привело к появлению новых угроз безопасности информации, возникновению новых форм и способов несанкционированного доступа к вычислительным ресурсам телекоммуникационных систем и сетей [1-4]. В частности, наибольшую уязвимость представляют применяемые методы сетевого управления, технологии доступа к предоставляемым сервисам и услугам, процессы мониторинга состояния телекоммуникационных систем и сетей. Под воздействием вредоносного программного обеспечения отдельные коммуникационные и вычислительные компоненты могут быть переведены в несанкционированные режимы функционирования, приводящие к сбоям, различным нарушениям установленного порядка их использования, уничтожению, искажению, блокированию, несанкционированной утечки обрабатываемой и передаваемой информации, а также к нарушению работы методов и алгоритмов маршрутизации между узлами телекоммуникационной системы [2-4]. Следовательно, разработка и иссле-